proofpoint

DATA SHEET

Proofpoint Account Takeover Protection

Detect, investigate, and respond to multistage account takeover

Key Highlights

- **Detect multistage account compromise with high precision**
- **Accelerate investigations with unified visibility across the attack lifecycle**
- **Reduce attacker dwell time through automated response and remediation**
- **Minimize fraud, data loss, and business disruption from compromised accounts**
- **Strengthen defense-in-depth with Proofpoint Collaboration Security Prime**

Proofpoint Account Takeover Protection helps organizations detect, investigate, and contain compromised user accounts across the entire account takeover (ATO) lifecycle—from pre-access indicators and successful compromise to post-access attacker activity.

Powered by Proofpoint Nexus® AI and threat intelligence, Account Takeover Protection delivers high-confidence detection of confirmed account compromise while providing complete visibility into attacker behavior. Security teams can quickly understand the scope of an incident, speed up investigations, and contain threats before they escalate into business email compromise (BEC), data theft, lateral movement, or other business-impacting attacks.

As part of Proofpoint Collaboration Security Prime, Account Takeover Protection integrates with Threat Protection Workbench and Threat Interaction Map to extend investigations beyond a single compromised account. By correlating identity compromise with email threats, user interactions, and attacker activity, it helps security teams gain a broader understanding of the attack campaign. This enables faster investigations, more informed response decisions, and stronger remediation.

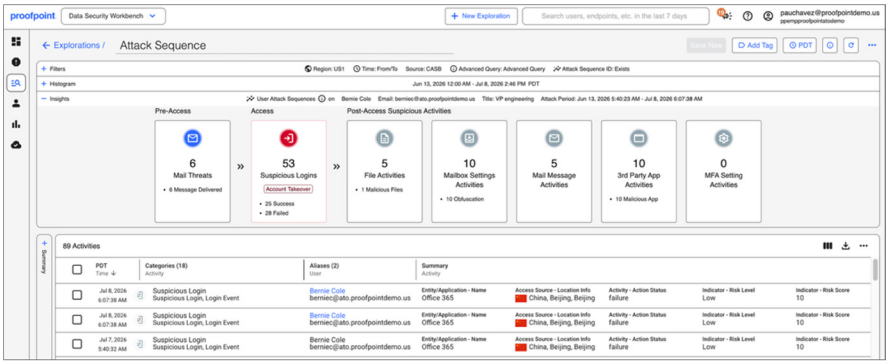

Figure 1. Gain comprehensive visibility across the ATO attack lifecycle from pre-access to post-access activities.

High-Confidence ATO Detection

Powered by Proofpoint Nexus AI, Account Takeover Protection delivers high-confidence detection of confirmed account compromise across Microsoft 365, Google Workspace, and Okta.

By continuously analyzing user activity across the account takeover lifecycle—from pre-access indicators through post-access attacker behavior—Account Takeover Protection identifies confirmed compromise with high confidence and prioritizes detections based on risk severity (Critical, High, and Medium). Each detection includes the behavioral indicators and evidence that contributed to the finding, helping analysts to quickly understand why an account was identified as compromised, prioritize response efforts, and take action with confidence.

Automated Threat Response

Account Takeover Protection helps organizations rapidly contain active threats through automated remediation actions that disrupt attacker access and accelerate recovery. Response actions include forcing password changes, resetting user passwords, revoking active user sessions, removing malicious mailbox rules, revoking unauthorized third-party OAuth applications, and other remediation measures that are designed to eliminate attacker persistence and restore account integrity.

By automating critical containment actions, security teams can reduce attacker dwell time, limit lateral movement, minimize business disruption, and accelerate recovery from account compromise.

Complete Attack Visibility

Once account compromise is confirmed, Account Takeover Protection provides complete visibility into the attack sequence, enabling security teams to understand how the attack unfolded and what the attacker did after gaining access.

Comprehensive forensic insights reveal post-access activities—including mailbox manipulation, malicious inbox rules, OAuth abuse, privilege changes, internal phishing, suspicious email activity, and persistence techniques. This helps analysts quickly determine the scope, sophistication, and reach of the attack. By reconstructing the attack sequence and highlighting affected users and assets, Account Takeover Protection helps accelerate investigations, supports more informed response decisions, and improves remediation.

Defense-in-Depth with Collaboration Security Prime

As part of Proofpoint Collaboration Security Prime, Account Takeover Protection extends beyond account compromise to deliver coordinated protection across the entire human attack lifecycle. While Account Takeover Protection detects, investigates, and contains compromised accounts, Prime enhances protection by preventing threats before compromise, correlating attacks across email and collaboration channels, improving user behavior through adaptive education, and providing unified investigation and response through Threat Protection Workbench and Threat Interaction Map.

Together, these capabilities support a defense-in-depth strategy that helps organizations prevent attacks, mitigate active threats, strengthen user resilience, and continuously improve their security posture from a single integrated platform.

Learn more at **proofpoint.com**

proofpoint.